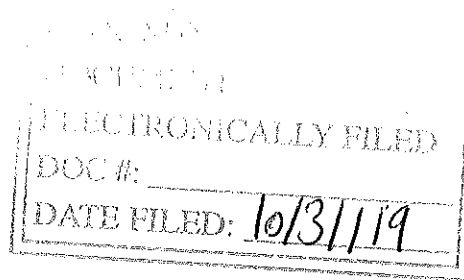


UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
 UNITED STATES OF AMERICA,

 -against-

 JOSHUA ADAM SCHULTE,

 Defendant.
 -----X

S2 17 Cr. 548 (PAC)

OPINION & ORDER

HONORABLE PAUL A. CROTTY, United States District Judge:

Joshua Schulte has been charged with stealing national defense information from the Central Intelligence Agency (“CIA”) and transmitting it to WikiLeaks.¹ Schulte moves to suppress evidence that he claims is invalid under the Fourth Amendment because the warrant application intentionally or recklessly misrepresented numerous material facts requiring suppression under *Franks v. Delaware*, 438 U.S. 154 (1978). (Def. Mot. To Suppress, Dkt. 108.) Schulte also requests an evidentiary hearing pursuant to *Franks*. (Def. Mem., Dkt. 109.) The Government opposes the motion to suppress and the request for a *Franks* hearing. (See Gov Opp’n, Dkt. 120.)

The Government search obtained evidence pursuant to the March 13, 2017 Warrant (“Home Evidence Warrant”) and the Child Pornography Warrants dated April 14, 2017 and May 10, 2017.² Schulte argues the Home Evidence Warrant is based on an affidavit that was replete

¹ On July 25, 2019, the Court granted Schulte’s motion to sever Counts One through Eleven of the Second Superseding Indictment, which involve allegations of theft and transmission to WikiLeaks, from Counts Twelve through Fifteen, which involve allegations of child pornography and copyright infringement. Dkt. 117.

² The Court will not hold a *Franks* hearing or suppress evidence related to the child pornography warrants. The Court has severed the child pornography counts. Further in response to the Government’s argument that it is improper to exclude the pornography evidence under the inevitable discovery doctrine, the Defendant conceded that

with misstatements, including *among others* that: (1) Schulte was “one of only three employees with authorized access to the information;” (2) the classified information was taken on March 7-8, 2016; (3) Schulte was the only one of the three employees with access whose name was not publicly disclosed by Wikileaks; and (4) Schulte regained unauthorized access to a project identified in the Wikileaks disclosure publication. (Def. Mem. at 16-17, Dkt. 109.)

The Court finds that neither a hearing under *Franks* nor suppression of the evidence is required because the Donaldson Affidavit supports a finding of probable cause, even without the alleged misstatements. The Court DENIES the motion to suppress.

BACKGROUND

On March 7, 2017 (“March 7 Leak”), Wikileaks made a series of disclosures that allegedly published classified CIA information. The Federal Bureau of Investigation (“FBI”) immediately began investigating after Wikileaks’s first disclosure. Six days later, on March 13, 2017, the FBI applied for a warrant authorizing a covert search of Schulte’s New York City apartment and electronic media. Special Agent Jeff D. Donaldson (“Donaldson”) of the FBI authored the affidavit in support of the March 13, 2017 Warrant. (*See* Donaldson Affidavit, Dkt. 111-1.) Donaldson stated he was an experienced counterespionage investigator and has worked in counterespionage since 2010. (*See id.* ¶ 1.) He described the March 7 Leak: Wikileaks published what it claimed were more than 8,000 documents and files containing classified information belonging to the CIA. (*Id.* ¶ 7.) Wikileaks’ press release claimed that the dissemination of the Classified Information was “the largest ever” unauthorized publication of classified CIA documents and constituted the “first full part” of a series. (*Id.* ¶ 7.) Donaldson

the Court “need not decide whether suppression of the child pornography evidence would be required based on the improper child pornography warrants alone.” (Def. Reply at 22.)

stated that the information published by Wikileaks was classified CIA information at the time of disclosure. (*Id.* ¶ 7.)

A. Method & Timing of Exfiltration

The affidavit described the likely timing and method of exfiltration of the March 7 Leak. According to the affidavit, the leaked materials were stored on a specific computer network (the Local Area Network or “LAN” network) within the CIA and used exclusively by a particular group within the CIA. (*Id.* ¶ 9.) The LAN is an isolated network, “physically separated (or ‘air-gapped’)” from the public internet, and accordingly it cannot be accessed from the public internet, but rather only through computers that are physically connected to the LAN. (*Id.*) Donaldson assessed that the March 7 Leak was likely copied from the LAN’s server that was used to store back ups (the “Back-Up Server”). (*Id.* ¶ 10.) Donaldson stated that the March 7 Leak information was likely stolen in or around March 7 or March 8, 2016. (*Id.* ¶ 13(a)-(d).) He noted in a footnote, however, that the timing assessment was based on “preliminary analysis” and that it was possible the information was copied later than March 8. (*Id.* ¶ 8(c)(iii) n.1.) According to the affidavit, the LAN system “was designed so that only those employees who were specifically given systems-administrator access could access the Back-Up Server” and as of March 2016, Joshua Schulte was one of three Systems Administrators. (*Id.* ¶¶ 11-12.)

Donaldson stated that Schulte was employed as a computer engineer by the CIA from May 2010 until November 2016 and was a member of the specific CIA group that exclusively used the LAN network. (*Id.* ¶¶ 12(a).) During Schulte’s six-year employment at the CIA, his responsibilities included developing computer code for projects, including projects described in the March 7 Leak. (*Id.*) According to the affidavit, Schulte has a skill set “that enabled him to write computer code designed to clandestinely copy data from computers.” (*Id.*) Donaldson

stated that based on a “preliminary review” the March 7 Leak appeared to contain the names and/or pseudonyms of the other two system administrations, but not Schulte’s name or pseudonym. (*Id.* ¶¶ 12(b).)

Donaldson added that Schulte was at work on the alleged date of the theft (i.e., March 7-8, 2016) with access to the relevant system. (*Id.* ¶ 13(a)(ii).) Further the affidavit stated that March 8, 2016 was the date of Schulte’s CIA Group’s offsite management retreat for many of the group’s senior and midlevel managers and thus, “much of the CIA Group’s management, including some to whom Schulte reported, were not present in the CIA component building where Schulte worked.” (*Id.* ¶ 13(b).) The employees attending the offsite included two of three employees who had direct line-of-sight to Schulte’s desk and computer. (*Id.* ¶ 13(a)-(b).) Moreover, at least one of the other two systems administrators also attended the CIA offsite and thus, did not have LAN access, while Schulte and the third administrator had LAN access. (*Id.* at ¶ 13(d).)

B. Schulte’s Unauthorized Actions at the CIA

In the affidavit, Donaldson described certain unauthorized actions taken by Schulte while employed by the CIA in April and May of 2016, which resulted in CIA management reprimanding Schulte. On or about April 4, 2016, around the time the CIA reassigned Schulte to another CIA branch, many of Schulte’s administrator privileges were revoked, including his permissions as a Systems Administrator on the LAN and his access to Project-1 highlighted by name in the March 7 Leak. (*Id.* at ¶ 15-16.) Schulte logged onto the CIA Group’s LAN without authorization and reinstated his own privileges. (*Id.*) Additionally, Schulte officially requested reinstatement of his access to Project-1, and before receiving a response, requested access to Project-1 from another employee. (*Id.*) Once granted access, Schulte without authorization

revoked computer access permission of all other CIA group employees to work on Project-1.
(*Id.*)

C. Complaints raised by Schulte while at the CIA

Donaldson explained that Schulte came to the CIA security's attention around March 2016 after Schulte alleged another co-worker threatened him. (*Id.* at ¶ 17.) Schulte expressed deep unhappiness about the CIA's response to the threat and threatened legal action against the CIA for its handling of the situation. (*Id.*) Schulte repeatedly stated that he felt CIA management was punishing him for reporting the threat incident and threatened that he or his lawyer would go to the media. (*Id.*) Additionally, the CIA learned Schulte had removed an internal CIA document about the threat incident despite being told not to do so. (*Id.*)

In August 2016, as part of a standard background reinvestigation of Schulte to renew his security clearance, the CIA conducted interviews with his CIA group colleagues. (*Id.* at ¶ 18(a)-(c).) According to the affidavit, "[s]ome (but not all) colleagues independently reported that Schulte's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worst in or around February 2016." (*Id.*) Multiple colleagues stated that Schulte had indicated he felt aggrieved by the CIA in a number of respects. (*Id.*) Some also reported they believed Schulte untrustworthy and potentially subject to outside coercion. (*Id.*) The affidavit noted "[o]ther colleagues made no such report, and indeed affirmatively reported that they believed Schulte was, in fact, trustworthy." (*Id.*)

D. Schulte's Resignation

Schulte resigned from the CIA in November 2016. (*Id.* at ¶ 19(a)-(c).) Schulte drafted a resignation letter that he never sent. (*Id.*) According to the affidavit, the letter began by stating that Schulte "had 'always been a patriot' and would 'obviously continue to support and defend this country until the day [he] died,' but that 'from this day forward' he would 'no longer do so

as a public servant.” (*Id.*) Schulte’s resignation letter “expressed concerns, including concerns about the network security of the CIA Group’s LAN network.” (*Id.*) The letter explained that Schulte felt the CIA ignored issues he raised about security, and attempted to conceal these practices from senior leadership, including that the CIA Group’s LAN was “incredibly vulnerable” to the theft of sensitive data. (*Id.*)

E. Schulte’s Conduct After the March 7 Leak

According to the affidavit, Schulte repeatedly contacted former co-workers (i.e., CIA employees) after the leak and asked about the investigation into the March 7 Leak. (*Id.* at ¶ 20(a)-(f).) Schulte repeatedly denied any involvement in disclosing classified information. (*Id.*) Schulte indicated that he believed he was a suspect in the investigation of the leak. (*Id.*) Based on conversations with Homeland Security, Donaldson stated that Schulte had a planned trip out of the country departing on March 16, 2017. (*Id.* at ¶ 21.)

F. Procedural History

Based on the Donaldson Affidavit, the magistrate judge issued the March 13, 2017 warrant and FBI agents searched Schulte’s Residence. After the initial warrant, the FBI executed a series of warrants authorizing the imaging of Schulte’s electronic devices, including the March 14, 2017 warrant, April 10, 2017, and May 10, 2017 warrants.

On September 6, 2017, the Government indicted Schulte on child pornography grounds. Nine months later, in June 2018, the Government filed a superseding indictment adding charges for theft and disclosure of classified information. On, September 18, 2018—over a year-and-half after the initial warrant issued—the Government provided a *Brady* Disclosure Letter to Schulte identifying statements in the Donaldson Affidavit that were not correct. The *Brady* Letter noted that, based on additional Wikileaks publications, it had developed further information relevant to

statements in the Donaldson Affidavit, which was not available at the time of the initial warrant. The *Brady* Letter acknowledged that the classified information was not stolen on March 7 or March 8, 2016, “at least five” employees had access to the specific part of the system where the classified information was likely stored, Schulte was not a Systems Administrator for the Back-Up system, and the project that Schulte accessed without authorization was not the project implicated by the Wikileaks publication.

DISCUSSION

I. The Suppression Motion

A. *Franks* Standard

The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. There is a “presumption of validity with respect to the affidavit supporting a warrant.” *Franks*, 438 U.S. at 171. In limited circumstances, however, “a defendant may challenge the truthfulness of factual statements made in the affidavit, and thereby undermine the validity of the resulting search or seizure.” *United States v. Awadallah*, 349 F.3d 42, 64 (2d Cir. 2003).

Under the *Franks* doctrine, the Fourth Amendment mandates a hearing if the defendant makes a “substantial preliminary showing” that (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the judge's probable cause finding. *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998). The *Franks* standard is a high one and such hearings are rare. *See e.g., United States v. Melendez*, No. 16CR33-LTS, 2016 WL 4098556, at *7 (S.D.N.Y. July 28, 2016). To obtain an evidentiary hearing, a defendant’s attack “must be more

than conclusory” and the “allegations must be accompanied by an offer of proof.” *Franks*, 438 U.S. at 171. “[I]f these requirements are met, and if, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required.” *Id.* at 171–72; *see e.g., Salameh*, 152 F.3d at 114.

1. Reckless Disregard

In *United States v. Rajaratnam*, 719 F.3d 139, 153 (2d Cir. 2013), the Second Circuit held that a subjective test governs the recklessness inquiry. One “recklessly disregards” the truth when one makes allegations while entertaining serious doubts about the accuracy of those allegations. *United States v. Vilar*, No. S305CR621KMK, 2007 WL 1075041, at *26 (S.D.N.Y. Apr. 4, 2007). “Because states of mind must be proved circumstantially, a factfinder may infer reckless disregard from circumstances evincing obvious reasons to doubt the veracity of the allegations.” *Rajaratnam*, 719 F.3d at 154 (quoting *United States v. Whitley*, 249 F.3d 614, 621 (7th Cir. 2001)). While under *Franks*, false assertions and omissions are governed by the “serious doubt” standard, “as a practical matter ‘the affirmative inclusion of false information in an affidavit is more likely to present a question of impermissible official conduct than a failure to include a matter that might be construed as exculpatory.’” *United States v. Mandell*, 710 F. Supp. 2d 368, 374 (S.D.N.Y. 2010) (quoting *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990)).

2. Necessity

“To determine if the false information was necessary to the issuing judge’s probable cause determination, i.e., material, ‘a court should disregard the allegedly false statements and determine whether the remaining portions of the affidavit would support probable cause to issue

the warrant.” *United States v. Canfield*, 212 F.3d 713, 718 (2d Cir. 2000)). If the corrected affidavit supports probable cause, the inaccuracies were not material to the probable cause determination and suppression is not required. *Rajaratnam*, 719 F.3d at 146.

B. Probable Cause

“Once the inaccurate information has been removed from the affidavit, the remaining portions of the affidavit should be reviewed *de novo* to determine if probable cause still exists.” *Canfield*, 212 F.3d at 718. In *Illinois v. Gates*, 462 U.S. 213, 232 (1983), the Supreme Court explained that “probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” In considering a request for a search warrant, the “task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit ... there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Id.* at 238. In assessing probable cause, courts consider the “totality of the circumstances.” *Id.*

II. Analysis

A. Suppression Under *Franks*

The Donaldson Affidavit contains several incorrect factual statements, which the Government disclosed in September 2018. Of particular concern are the incorrect statements about the number of people who had access to the leaked information (one of three to more than five) and the alleged date of the theft (March 7-8, 2016 to April 20, 2016). Still, a *Franks* hearing is required only if the Government’s incorrect statements were necessary to the magistrate’s determination of probable cause. Thus, the Court considers whether, based on the record before the magistrate judge, and disregarding the challenged material, there was sufficient

evidence to find probable cause without the incorrect statements. *See Franks*, 438 U.S. at 171-72; *United States v. Rajaratnam*, No. 09 CR 1184 RJH, 2010 WL 4867402, at *11 (S.D.N.Y. Nov. 24, 2010); *United States v. Kidd*, 386 F. Supp. 3d 364, 371 (S.D.N.Y. 2019).

Schulte argues that the remaining facts are not sufficient to support probable cause and were made with reckless disregard for the truth, and so the fruits of the FBI's search much be suppressed. (Def. Mem. at 18.) Schulte primarily basis his "necessity" argument on the fact that there are innocent explanations for his conduct. But "the fact that an innocent explanation may be consistent with the facts alleged...does not negate probable cause." *United States v. Fama*, 758 F.2d 834, 838 (2d Cir. 1985). Schulte's innocent explanations for his conduct may make certain evidence less compelling, but it does not eliminate its probative value. The standard for probable cause is "relaxed"; it does not require even a *prima facie* showing. *United States v. Martin*, 426 F.3d 68, 76 (2d Cir. 2005) (explaining the defect in the argument that "conflates evidence of probable cause to sustain a warrant with proof of a *prima facie* case," because "probable cause does not require a *prima facie* showing" of the crime).

Here, based on a close analysis of the Donaldson Affidavit, the Court determines that there is probable cause, even without the statements Schulte challenges. Excluding the challenged statements, the affidavit provides the following which is sufficient to determine that there is a "fair probability that contraband or evidence of a crime" would be found in Schulte's apartment on his electronic devices, Schulte: (1) had the necessary skills and unique access to the stolen information and LAN network, (2) had a deep understanding of the relevant CIA computer systems and information exposed by the Wikileaks, (3) had a motive to harm the CIA because he was angry that the CIA did not take his complaints seriously, (4) had threatened to go public previously, (5) had secured unauthorized access to Classified Information in violation of

CIA directives, (6) had drafted an email warning CIA management about security vulnerabilities that could expose information from the LAN that eventually was exposed by Wikileaks, and (7) demonstrated a guilty conscience. These facts support a conclusion that Schulte had both a motive and opportunity to take the classified CIA information. Further, the nature of the LAN network—an isolated network that cannot be accessed from the public internet—strongly suggests that the theft of classified information was an inside job and the information was believed to have been stolen using portable media given the substantial amount of data published. Finally, the affidavit contained an extensive discussion of the modus operandi of those who engage in espionage, including how such files are transferred, stored, and leave a lasting digital footprint. Taken together, these facts support a finding of probable cause to issue a search warrant.

The Court agrees that the misstatements make the warrant application stronger, but not in a way that defeats probable cause. The test does not require that culpability be established. “[T]o suffice for probable cause, it need not have been.” *Rajaratnam*, 2010 WL 4867402, at *11.

Disregarding the incorrect factual statements, the Court finds that the Donaldson Affidavit establishes probable cause. Since the incorrect statements were not necessary to the probable cause determination, neither a hearing nor suppression is required. *See Salameh*, 152 F.3d at 114 (district court did not err in denying a *Franks* hearing because the allegedly false statements were not necessary for a finding of probable cause).

B. Nexus & Staleness

Schulte also argues that the factual allegations were (1) insufficient to establish the requisite nexus to search his apartment and (2) stale. (Def. Mem. at 27–28.) According to

Schulte, there was no basis to conclude contraband would be found in his New York apartment given Schulte's computer expertise, his move from Virginia to New York, and the year-long period between the alleged theft of classified information and the application for the search warrant.

Schulte's nexus argument is unavailing. The Donaldson Affidavit identified the offense for which the FBI established probable cause, described the place to be searched, and specified the items to be seized. *See United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013). Contrary to Schulte's argument, the affidavit stated that Schulte likely stole the information by exfiltrating data onto a removable drive and then removed that drive from the CIA. Other facts in the affidavit supported this assertion, including that the LAN network was not accessible via public internet and the substantial amount of data stolen. Further, the affidavit added that such devices are often maintained in the individual's home and stated that transmitting such information often leaves a digital trace on electronic devices that can be forensically recovered even where the files were deleted. The Court determines that nexus has been established.

As to staleness, the two critical factors in determining staleness are the age of the facts alleged and the nature of the conduct alleged to have violated the law. *United States v. Ortiz*, 143 F.3d 728, 732 (2d Cir. 1998). Where, as here, the crime involves leaking classified information and the leak was published one week before the warrant issued, the basis for the search is not automatically stale where an affidavit alleges such information was gathered (or stolen) a year earlier. The nature of espionage provides that conduct may be ongoing because gathering or stealing classified information could have occurred long before the actual transmission. That the Government now posits—after a year of investigation—that Schulte transmitted the classified information months before the warrant issued is beside the point. (Def.

Mem. 30 n.6.) *See United States v. Wagner*, 989 F.2d 69, 75 (2d Cir. 1993) (the relevant question is whether “probable cause can be said to exist *as of the time of the search*”). The Donaldson Affidavit did not suggest that Schulte transmitted the classified information a year earlier; indeed, the affidavit provided facts suggesting ongoing publishing of classified CIA information by Wikileaks—i.e., the March 7 Leak constituted the “first full part” of a series. Thus, the FBI reasonably could have inferred that Schulte had transmitted classified information from his New York City apartment shortly before the initial Wikileaks publication and could have reasonably inferred that transmission was ongoing. *See Ortiz*, 143 F.3d at 732 (where the affidavit “presents a picture of continuing conduct or an ongoing activity,...” the passage of time between the last described act and the warrant application is less significant). As such, the Court rejects the argument that the showing of probable cause to search Schulte’s apartment and electronic devices is impaired by staleness.

CONCLUSION

For the reasons stated, the Court DENIES the Defendant’s motion to suppress. The Clerk of the Court is directed to terminate Docket 108.

Dated: New York, New York
October 31, 2019

SO ORDERED



PAUL A. CROTTY
United States District Judge